

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
KNOXVILLE DIVISION

FILED

DEC 07 2020

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
"BODAVIS1985")
THAT IS STORED AT PREMISES)
CONTROLLED BY SNAPCHAT, INC.)
)

Clerk, U. S. District Court
Eastern District of Tennessee
No. 3:20-MJ-2170
At Knoxville
JUDGE GUYTON

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A SEARCH WARRANT**

1. I, Paul A. Durant, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application for a search warrant to require Snapchat Inc. (hereafter "Snapchat") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Snapchat account that is stored at premises owned, maintained, controlled, or operated by Snapchat, a company located at 64 Market Street Venice, CA. The information to be disclosed by Snapchat and searched by the government is described in the following paragraphs and in Attachments A and B.

3. I am a Special Agent (SA) with the Johnson City Resident Agency (JCRA) of the Federal Bureau of Investigation (FBI), and have been since February 2020. I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am familiar with investigations and enforcement of federal child pornography laws in which electronic devices are used as the means for producing, transmitting, collecting and storing child pornography. I have knowledge criminals use electronic devices, such as mobile telephones, to store information related to criminal activity.

4. This affidavit is submitted in support of an application for a search warrant to search the Snapchat accounts listed in attachment A and items to be seized as described in Attachment B.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(5)(B) exist on the Snapchat account.

II. PROBABLE CAUSE

6. On June 23, 2020, an FBI Washington Field Office (WFO) task force officer (TFO) was acting as an online covert employee (OCE) as part of the Child Exploitation Task Force. The OCE made a case on a defendant. Pursuant to a defendant's consent the OCE conducted an account takeover of the defendant's social media accounts to include KIK instant messenger for the purpose of identifying other child predators. On June 23, 2020, a KIK user using the KIK name, "sia1825," later identified as Shana Coffey (COFFEY) entered a KIK screening room. This room is known to the OCE as a room where people enter and post child sexual abuse material (CSAM) for the purpose of being invited to join a private room to trade. The rules of the screening room require users to send 3 videos of CSAM to an administrator, among other things.

7. On June 23, 2020, at 7:41pm COFFEY entered the screening room and stated that she was a 40 year-old female from Tennessee. COFFEY initiated a private chat with the OCE via KIK stating, "3 vids?" The OCE asked COFFEY to hold up four fingers in front of her face to verify that she was female. COFFEY complied and sent the UC a live camera picture of herself holding up four fingers near her face. During the course of the chat COFFEY stated that she had an eight year-old daughter that resided with COFFEY. COFFEY made the following statements as it relates to her daughter, "I've touched some while she's sleeping and showed some pics and vids to get her curious."

8. During the course of the chat the OCE asked COFFEY, "U have a lot of stuff." COFFEY responded, "I've got a decent collection so far..always looking for new groups to find new stuff I haven't seen." COFFEY further stated, "Some pretty good ones of crying and forcing honestly." During the course of the chat COFFEY sent the OCE a live camera picture of her daughter. The picture depicted a chubby prepubescent girl wearing a light-colored T-shirt and white headphones. COFFEY stated, "she's very curvy for her age..little breast developing already."

9. During the course of the chat COFFEY stated that she met a guy on the whisper app and referred to him as "dom." COFFEY stated that she has given her daughter melatonin and allowed this person to masturbate, touch and ejaculate on her daughter while she was in a deep sleep. COFFEY stated, "I just have one pic of her little pussy I saved for him." COFFEY sent the OCE this picture. The picture depicts a close up shot of a prepubescent child's bare vagina. The picture solely focuses on the vagina and with the thighs visible. The child in the picture had the same chubby build as seen in the image COFFEY sent to the OCE previously.

10. The OCE asked COFFEY to take a picture of COFFEY holding up three fingers next to her daughter to confirm she had immediate access. COFFEY complied and sent the OCE an image of herself holding up three fingers in front of her daughter. The minor is wearing the same light colored shirt. COFFEY stated that she had a few more images of her daughter when she was a lot younger. COFFEY sent two images of her daughter to the OCE. The first image depicts a nude toddler child standing up holding a ball above her head. The second image depicts a toddler sitting naked with her legs crossed. COFFEY stated that she would ask her "dom" if he saved any additional images of her daughter.

11. During the course of the chat COFFEY sent the OCE five videos of CSAM. The first video depicts a prepubescent child being penetrated in the anus or vagina by an adult male penis, the child is crying. The second video depicts an adult male inserting his penis in the vagina of a prepubescent child. The third video depicts an adult male digitally penetrating a toddler girl's vagina with his fingers. The video also shows the male inserting his penis in the child's anus. The fourth video depicts an adult male having anal or vaginal sex with a prepubescent girl. The girl is heard crying saying, "no it hurts." The fifth video depicts a prepubescent child being vaginally penetrated by an adult

male. The child is heard screaming and crying. These videos do not depict COFFEY's daughter.

12. COFFEY stated that she has only allowed her "dom" to play with her daughter. COFFEY stated that they call her daughter "demon" as a code name for her. COFFEY stated that she exchanges child porn with her "dom" and also sends him videos of her masturbating next to her sleeping daughter.

13. On June 23, 2020, the images COFFEY sent the OCE of herself while using the KIK name "sia1825" were run through open source searches identifying a social media account in the name "Shana Coffey". Further commercial database searches for the name "Shana Coffey" in Tennessee yielded: Shana Coffey (DOB: 09/07/1979; SSN: 414-33-1337; TN DL: 086745674) that resided at 715 East Jefferson Street, Jefferson City, TN 37760. A social networking profile (www.facebook.com/scoffey79) was identified as belonging to COFFEY. Comparison of publicly available photographs on Facebook, as well as the identified driver's license photograph matched photographs sent to the WFO OCE by Kik username "sia1825." Additionally, publicly available photographs of COFFEY's daughter on Facebook matched photographs of the victim sent to the WFO OCE by Kik username "sia1825."

14. On June 24, 2020, this affiant received information regarding COFFEY from WFO. Utilizing subscriber information and IP addresses received from Kik, an exigent request for subscriber information was submitted to Verizon Wireless for IP addresses 174.196.8.55 and 174.195.7.30 also used in the KiK screening room. Both IP addresses came back with the following Subscriber information: Debra Hurst, 715 E Jefferson Street, Jefferson City, TN 37760. The same address as on COFFEY's driver's license.

15. An FBI TFO drove to 715 East Jefferson Street, Jefferson City, TN 37760 and located a black Nissan sedan in the driveway. A search of COFFEY's vehicle registration yielded a black Nissan Sentra license plate 7E79A0 registered in her name. The address listed on the black Nissan Sentra is 715 E. Jefferson Street, Jefferson City, TN 37760. The same address as on COFFEY's driver's license.

16. On June 26, 2020, the Johnson City FBI and local law enforcement executed a federal search warrant from the Eastern District of Tennessee Case No. 3:20 MJ-2149, at 715 East Jefferson Street, Jefferson City, TN 37760. While executing the search warrant COFFEY was located and interviewed by agents after being read her Miranda rights. During the interview COFFEY was shown

pictures and messages between the Kik user name, "sia1825" and the Kik OCE. COFFEY identified "sia1825" as her Kik user name. Initially, COFFEY stated that she did not send the messages and that the minor victim had access to her phone when the communication occurred with the OCE. COFFEY stated that the close-up picture of the prepubescent female's bare vagina sent to the OCE via "sia1825" was of COFFEY and not the minor. COFFEY later admitted that she was the one communicating on Kik with the OCE and the close-up picture of the prepubescent female's bare vagina was of the minor victim and not COFFEY. COFFEY also admitted to sending several nude images of her daughter. Further, COFFEY admitted sending videos containing CSAM to the OCE via Kik.

17. COFFEY stated that she received videos of CSAM from Timothy Beau Davis (DAVIS) whom she referred to as "dom." COFFEY said she met DAVIS through the whisper app, a social media application approximately six months ago. They exchanged social media information and began communicating on Snapchat and Kik instant messenger where they exchanged CSAM. COFFEY's cell phone was seized during the search warrant and the initial inspection revealed many active social media applications to include Snapchat.

18. On June 26, 2020, DAVIS was located and interviewed. DAVIS admitted to downloading CSAM from the internet. DAVIS stated that COFFEY asked him to find videos of younger kids having sex. DAVIS went on Kik and searched chat rooms to locate CSAM and sent it to COFFEY via Snapchat and Kik. DAVIS said that COFFEY wanted the CSAM so she could share them with her friends. COFFEY also asked DAVIS to have sex with the minor victim and tried to set up a day to meet. DAVIS told COFFEY he had to work because DAVIS did not want to meet up to have sex with the minor. DAVIS said that COFFEY had sent him pictures of the minor victim where she was nude, and he deleted the pictures after he received them. DAVIS consented to have his phone searched. Davis provided agents with his social media account user ids which included Snapchat account "Bodavis1985." During the search CSAM was found on his cell phone which was then seized and sent to the Knoxville FBI office to be examined.

19. On July 8, 2020, SA Durant received the forensic report for DAVIS's iPhone. The report stated that there were 154 images consistent with child pornography located on the device. Of those images, 141 were unique and 13 were duplicates. All of the images were located in the cache folder for

the application "Mega", a secure cloud storage application. Also found in the folder were two additional images of note. The first image displays the text "PEDO.PUZ." and the second image displays the text "make daddy cum 12yo". Additionally, DAVIS had shana0011 as a contact in his Snapchat contacts which was Shana Coffey's Snapchat user ID.

20. Based on my training and experience Snapchat may contain data no longer accessible on the physical device. Since the subject is unsure of the date they exchanged CSAM we are requesting data from 01/01/2019 to 07/31/2020. The information obtained from the accounts would help us locate additional victims and/or subjects associated with this case.

III. PRESERVATION LETTER

21. On June 26, 2020, the FBI issued a Preservation Letter to Snapchat for the account "Bodavis1985."

IV. SNAPCHAT

22. Based upon my knowledge, training, and experience, I have learned that Snapchat is a video messaging application for mobile devices. Snapchat was created in 2011 as part of a Stanford University class project. Users can take photos, record videos, add text and drawings, and send them to a controlled list of recipients. These sent photographs and videos are known as "Snaps." Users set a time limit for how long recipients can view their Snaps, after which they will be hidden from the recipient's device and deleted from Snapchat's servers.

23. Some of the features of Snapchat are as described below:

- a. Snaps: A user takes a photo or a video using the camera phone in real-time. The user then selects a time limit of 1 - 10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in a Snap.
- b. Stories: A user can also add the photo/video to their "Story." Depending on the User's privacy settings, the photos or videos added to a Story can be viewed by either all Snapchat users or just the user's friends for up to 24 hours.

- c. Chat: A user can also type messages to friends within Snapchat using the Chat feature. A user sends a chat message to a friend, and once it is viewed by both parties, and both parties swipe away from the Chat screen-the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that the user wants to keep. The user can clear the message by tapping it again.
- d. Memories: Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos or videos from their phone's photo gallery in memories. Content saved in Memories is backed up by Snapchat and may remain in Memories until deleted by the user.
- e. Location data: If a user has device level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending upon the purpose of the collection.
- f. User Name: Each Snapchat account has a user name and a display name. The Snapchat user name is a unique identifier associated with a specific Snapchat account and cannot be changed by the user. A display name, on the other hand, is not a unique identifier and can be created and changed by the user to indicate how the user will appear in the app.
- g. Quick Add: The Quick Add feature is a suggested friends list which identifies for Snapchat users a list of other users who might be friends with your friends on Snapchat. A user can add a friend from the Quick Add list without the other user accepting a friend request. However, the added friend is notified that their new friend added the user through the Quick Add feature.

24. Snapchat subscriber information includes user name, email address, date and time account created, IP address used to create the account, phone number, and display name. The email address and phone number are optional for users to input and are not verified in any way. Snapchat users can select different levels of privacy for the communications and information associated with their

Snapchat accounts. By adjusting these privacy settings, a Snapchat user can make information available to only himself or herself, to particular Snapchat users, or to all Snapchat users.

25. Social networking providers such as Snapchat typically retain additional information about their users accounts, such as information about the length of service, the types of service utilized, and the means and source of any payments associated with the account, in addition to stored electronic communications.

V. BACKGROUND ON CHILD SEXUAL ABUSE MATERIAL (CSAM)

26. Based upon my knowledge, training, and experience of investigations in child exploitation and child sexual abuse material, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced, distributed, and obtained.

27. As a result of my training and experience in child exploitation and child sexual abuse material investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the distribution and collection of child sexual abuse material.

- a. Child sexual abuse material collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Collectors of child sexual abuse material may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child sexual abuse material collectors often times use these materials for their own sexual arousal and gratification. Furthermore, they may use these materials to lower the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Child sexual abuse material collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. "Child Erotica", as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- d. Likewise, collectors of child sexual abuse material often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area.
- e. Child sexual abuse material collectors also may correspond with and/or meet others to share information and materials; are rarely able to completely destroy correspondence from other child sexual abuse material distributors/collectors; conceal correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child sexual abuse material.
- f. Collectors of child sexual abuse material prefer not to be without their child sexual abuse material for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child sexual abuse material throughout the world.
- g. Individuals involved in the trade of child sexual abuse material often use specialized software to conceal the existence of evidence and/or destroy said evidence. There are a variety of different programs that an individual can use to accomplish these objectives,

many of which are free. Additionally, child abusers have been known to store child sexual abuse material in unconventional locations on a computer or mobile phone.

- h. Often times, collectors of child sexual abuse material will download and store images and communications of children they known or with whom they have communicated. These images many not necessarily be pornographic or obscene in nature, however they are often used for their own sexual gratification.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VII. CONCLUSION

29. I respectfully request that the attached warrant be issued authorizing the search of the Snapchat ids described in Attachment A and seizure of the items described in Attachment B.

Respectfully submitted,



Paul A. Durant
Special Agent
Johnson City Resident Agency (JCRA) of the
Federal Bureau of Investigation

Sworn to and subscribed before me
this 21st day of July, 2020.



H. BRUCE GUYTON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the accounts “Bodavis1985” that is stored at premises owned, maintained, controlled, or operated by Snapchat Inc., a company located at 64 Market Street Venice, CA

ATTACHMENT B

Particular Things to be Seized

For the time period of 01/01/2019-07/31/2020

I. Information to be disclosed by Snapchat

To the extent that the information described in Attachment A is within the possession, custody, or control of Snapchat, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Snapchat, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

1. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
2. All records or other information regarding the devices associated with, or used in connection with, the account or any devices used to access Snapchat services, including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");
3. The contents of all messages associated with the account from 01/01/2019 - 07/31/2020 including stored or preserved copies of messages sent to and from the account (including all draft and deleted messages), the source and destination account of each message, the date and time at which each message was sent, the size and length of each message, the actual IP addresses of the sender and the recipient of each message, and the media, if any, attached to each instant message;
4. All activity, connection, and transactional logs for the account with associated IP addresses
5. All records and information regarding locations where the account or devices associated with the account were accessed
6. All records pertaining to the types of service used;
7. All records pertaining to communications between Snapchat and any person regarding the account, including contacts with support services and records of actions taken; and
8. All files, keys, or other information necessary to decrypt any data produced in an encrypted form.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(5)(B) involving DAVIS since 01/01/2019 including, for each account listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Snapchat id, including records that help reveal the whereabouts of such person(s);
- b. Photographs, images and video, including but not limited to, sexually explicit photographs of minors.
- c. Files depicting sexual conduct involving minors or persons who appear to be minors.
- d. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- e. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.
- f. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- g. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.